REMARKS

Claims 11, 13, 14, 16-19, and 22-28 are pending. The Examiner's reconsideration of the rejection in view of the amendments and remarks is respectfully requested.

By the Advisory Action the objections and rejection under 35 USC 112 has been withdrawn.

Claims 11 and 13-22 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Ober et al. (USPN 6,397,331) in view of Morgan et al. (USPN 6,185,685). The Examiner stated essentially that the combined teachings of Ober and Morgan teach or suggest all of the limitations of Claims 11 and 13-22.

Claims 11 and 22 are the independent claims.

Claims 11 and 22 claim, *inter alia*, "reading a certificate including a first public key into a protected memory; validating said certificate with a second public key permanently stored on said processor; reading a signed authorized code into said protected memory, wherein said protected memory is cryptographically protected; preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first public key."

Ober teaches a method of expanding a secure kernel memory area to accommodate additional software code (see Abstract). Ober does not teach or suggest "reading a certificate including a first public key into a protected memory; validating said certificate with a second public key permanently stored on said processor" as claimed in Claims 11 and 22. Ober teaches that a secure kernel memory area may be expanded into an unprotected memory area (see col. 2, lines 28-34). Further, Ober requires that a kernel extension be signed by a trusted authority before it can be down loaded into the newly acquired memory (see col. 2, liens 55-60). Ober fails to teach or suggest validating the trusted authority, much less, validating said certificate including a first public key with a second public key permanently stored on said processor, essentially as claimed in Claims 11 and 22.

Further, nowhere does Ober teach or suggest that protected memory is cryptographically protected – for example, Ober's cryptographic algorithm stored in the newly acquired memory is not itself cryptographically protected. The data stored in the newly acquired memory of Ober is merely signed (see col. 2, liens 58-60). With regards to the Examiner's suggestion on page 3 of the Final Office Action that digital signing is a type of cryptographic protection, Applicants believe that digital signing is a type of cryptographic protection only to the extent of the creation of the signature itself, as no data is encrypted as the result of a digital signature - digital signatures are cryptographic creations used to verify authenticity of data, not to encrypt data. Therefore, Ober fails to teach or suggest "reading a signed authorized code into said protected memory, wherein said protected memory is cryptographically protected" as claimed in Claims 11 and 22.

Morgan teaches a system of servers and clients which exchange symmetric keys for implementing a multi-stage login (see Abstract and FIG 2A). Morgan does not teach "reading a certificate including a first public key into a protected memory; validating said certificate with a second public key permanently stored on said processor" as claimed in Claims 11 and 22. Morgan teaches that a public key is encrypted, using a hash value as a symmetric key prior to a key exchange (see col. 8, lines 66-67 and FIGS 2A and 3A). The public key is used in symmetric encryption and not in verification of code. Thus, Morgan's encryption of a public key is not believed to be analogous to validating a certificate including the public key, wherein the public key is used to verify a signed authorized code, essentially as claimed in Claims 11 and 22. Therefore, Morgan fails to cure the deficiencies of Ober.

The combined teachings of Ober and Morgan teach an encrypted public key stored in an expanded secure kernel memory area. The combined teachings of Ober and Morgan do not teach or suggest "reading a certificate including a first public key into a protected memory; validating said certificate with a second public key permanently stored on said processor" as claimed in Claims 11 and 22.

Claims 13, 14, 16-19 depend from Claim 11. The dependent claims are believed to be allowable for at least the reasons given for Claim 11. Claims 15, 20 and 21 have been cancelled. The Examiner's reconsideration of the rejection is respectfully requested.

Claim 23 claims, *inter alia*, "a processor in signal communication with said protected memory for preparing to execute said signed authorized code from the protected memory by verifying that a digital signature contained in of said signed authorized code is original in accordance with a first public key stored in said protected memory and validated by a second public key permanently stored on said processor, and if said original digital signature is verified, then branching to a copy of said authorized code in said protected memory to begin execution."

For at least the reasons given for Claims 1 and 11 above, the combined teachings of Ober and Morgan do not teach or suggest "a processor in signal communication with said protected memory for preparing to execute said signed authorized code from the protected memory by verifying that a digital signature contained in of said signed authorized code is original in accordance with a first public key stored in said protected memory and validated by a second public key permanently stored on said processor" as claimed in Claim 23. For example, the combined teachings of Ober and Morgan teach an encrypted public key stored in an expanded secure kernel memory area. The encrypted public key in a secure kernel memory area is not believed to be analogous to a second public key permanently stored on a processor for validating a certificate including a first public key, essentially as claimed in Claim 23.

Accordingly, Claim 23 is believed to be in condition for allowance. Claims 24-28 depend from Claim 23 and are believed to be allowable for at least the reasons given for Claim 23.

For the forgoing reasons, the application, including Claims 11, 13, 14, 16-19, and 22-28, is believed to be in condition for allowance. Early and favorable reconsideration of the case is respectfully requested.

Respectfully submitted,

Dated: July 23, 2007

/Nathaniel T. Wallace/
Nathaniel T. Wallace
Reg. No. 48,909
Attorney for Applicants

F. CHAU & ASSOCIATES, LLC
130 Woodbury Road
Woodbury, New York 11797
TEL: (516) 692-8888
FAX: (516) 692-8889